Knowledge management for modelling nuclear power plants control in incidental and accidental states

Pierre Millerat, Jean-Louis Ermine, Mathias Chaillot

Computational Engineering in Systems Applications, CESA'96 IMACS Multiconference, Lille, July 9-12, 1996, Symposium on Modelling, Analysis and Simulation, Vol. 2, pp. 982-987.

French version

« Application de la systémique à la conception d'un modèle de conduite en mode dégradé d'une centrale nucléaire »

3ième Congrès Européen de Systémique, Rome, 1-4 octobre 1996, pp. 1011-1017, Kappa Ed.

Knowledge management for modelling nuclear power plants control in incidental and accidental states

Pierre Millerat[*], Jean-Louis Ermine[**], Mathias Chaillot[**]

[*] *EDF/DER/CCC*
Groupe Études Fonctionnelles
6 quai Wattier
78401 Chatou Cedex, France

[**] *Commissariat à l'Énergie Atomique*
DIST/SMTI
Groupe Gestion des Connaissances
Centre d'Études de Saclay
91191 Gif sur Yvette Cedex

Mathias.Chaillot@cea.fr
jlermine@tabarly.saclay.cea.fr

1. Introduction

1.1. Project environment

The project summarised in this article has been managed in the context of the EPR: European Project Reactor. This is a very large project involving especially the German company Siemens, the French company Framatome and the French national power supplier EDF (Électricité de France). The aim of that project is to design the next generation of nuclear power plants (NPP) in order to make them safer, and to integrate a lot of advanced technologies. The French part of the EPR, the REP 2000 project, involves EDF and CEA (Commissariat à l'Énergie Atomique), which is the French atomic research organisation.

A small part of EPR is dedicated to control command and man machine interface, especially to intelligent computerised systems for operators. The project below addresses a part of that question.

1.2. Project objectives

The two main objectives of the project are:

*) *Knowledge capitalisation* : to integrate the huge amount of knowledge accumulated by EDF during those last twenty years on safety, summarised in the APE (Approche Par Etats, State-oriented Approach), methodology which is an approach based on the continuous analysis of the plant state, not involving the plant history.

*) *Complexity management*: to build a model of the plant control in incidental and accidental states enabling:

1) To understand the control actions related to the physics processes actually taking place in the plant
2) To explain every control task in relation with the process it controls
3) To put every control task in the general context of operator's activity

Hence, the result of the project is a model (in fact several models), built according to a knowledge management methodology, describing several pertinent point of views on plant control, based on APE. This model fulfils the above requirements, and then can be used for training the operators to incidental and accidental situations. To facilitate the consultation of this model, hypermedia software has been implemented.

2. The knowledge management method

2.1. The modelling levels

MKSM (Methodology for Knowledge Systems Management) [Ermine 96] has its origin in research and applications within the French Atomic Agency (CEA). It offers an analysis process addressing, at least partially, the mastering of complexity in knowledge management projects, before considering an "operational" application. The method has several refining steps for analysing and modelling the knowledge system, down to the sufficient grain that gives a correct visibility over the knowledge to be managed, the possible projects and the pertinent decision criteria.

MKSM is designed for general purposes in knowledge management, from strategic knowledge management to operational projects as expert systems, information retrieval systems, and documentation or assurance quality. The challenge in this project is to use the general modelling techniques of MKSM for the specific objectives described above: are those techniques adequate to capture knowledge on NPP control, are the models sufficient to validate the APE methodology?

MKSM proposes several modelling phases, depending on the "knowledge grain" which is to be considered. It considers three different levels. The first one is the contextual level, where the knowledge system is analysed and modelled in its context, the modelling techniques are relevant to systemic and functional analysis. The second level is the cognitive level, where emphasis is put on the semantic structures of knowledge, particularly the problem solving methods used by the specialists to operate the process, the modelling techniques at this level are relevant to knowledge engineering. The third level is the information level, relevant to usual information technologies.

The project has focused essentially on the first level, which seemed, in that problem, the most difficult to capture. The question answered is : what are, according to APE, the general activities performed in the NPP management in incidental and accidental states, and what for ?, (i.e. what are the phenomena in the NPP involved in those activities ?). In the MKSM vocabulary, it means to build the *activity model* and the *domain model* and to link them. Regarding the second level, cognitive modelling has been used as a feasibility study to point out that the contextual models can be linked to the usual operator's know-how, that is to say the control procedures written in the guidebooks available in the NPP control command room. Procedures have been modelled in a conceptual language, describing the strategy used to solve the problem of incidental and accidental management. In the MKSM vocabulary it means to build the *task model* (it is a usual modelling technique in classical knowledge engineering, see for instance [Hickman 89], [Breuker 94]).

We turn now to describe how are built the three quoted models in MKSM. Examples will be given in the NPP control application.

2.2. The MKSM models

2.2.1. The domain model

The domain model intends to answer the question : what is the knowledge about ? The basic hypothesis of that modelling phase is that the domain is described by the set of processes which take place in it. The domain model is then a model defining and describing processes. MKSM, in that purpose, makes use of the general system theory, as exposed for instance in [Le Moigne 77]. This theory is based on two fundamental dualities . The first one is the *flow/field duality*. Every process emits a flow, which is characteristic of the process, usually classified in flow of matter, energy or information (classification that can be easily extended). The notion of flow is strongly attached to the notion of field, and cannot be separated. The field can be seen as an "influence capacity". It represents the set of elements which can influence the process, but which is not part of it. It is a well known notion in physics, which can be easily generalised. This is the case for instance of a catalyst in a chemical reaction, the weather conditions in a fire, the legal rules in a hazardous process etc. To summarise, the flow is part of the active process and field is part of the active environment. The second duality is the *source/target duality*. In a process, the flow is considered as flowing from a source to a target, which is both sub-systems specific to the described process. The sub-system, source or target, is described as composed of a material support (source or target system), and an action which is either at the origin of the flow (source action) or at the end of the flow (target action). The model is completed with the *triggering events*, which are activating the process and are at the temporal origin of the flow, and the external *consequences* of the impact of the flow on the target. This model (Source/Target/Flow/Field) provides a useful qualitative description of phenomena in various domains as physics, chemistry, biology... The modelled processes can be linked with causality links or chaining links to provide a graph of scenarios, which completes the domain model of MKSM. It is often added a set of analytic notices, written by experts, giving scientific or quantitative elements useful to the understanding of the processes (mathematical equations, chemical formulas...).

2.2.2.The activity model

The activity model describes the system activity which produces or utilises the knowledge, and put the domain knowledge (described in the processes) in an operational context. It is built by a "top-down" analysis, similar to a functional analysis, where each activity is decomposed in a hierarchy of lower sub-activities. This analysis is data-driven, and the obtained model is a simple description of the activities (the system "functions") linked by data flows. The modelling language is classical, adapted from usual DFD (Data Flow Diagrams) as SADT for instance. The processes of the domain model are included in the data flows in three possible ways. A process can be used as a knowledge resource (its knowledge is necessary or useful to perform the activity), a process can be triggered or inhibited by an activity.

2.2.3. The task model

The task model is a cognitive model in the sense of cognitive ergonomics for instance, ([Scapin 90] or [Sebillotte 88]). It describes the strategy used to solve the problem(s) in the considered knowledge system. It is the description of problem solving methods, as often used in knowledge engineering, answering two types of questions : "what are the tasks to achieve ?" and "how generally do we achieve this kind of tasks ?". The task model of MKSM builds the description of the tasks ordering to be performed, by means of a tree decomposition which recursively refines the different tasks in sub-tasks, until terminal tasks. Each composed task has a type, specific of the control it has on its sub-tasks : a task can be sequential, alternative, repetitive, parallel... The task tree given by the model is the control flow of the expressed knowledge (the dynamic knowledge). In that project, the task model has been used to describe the control procedures of the operators.

3. The modelling activities

3.1. Principles of modelling

Any model of plant control requires an important knowledge on plant activity. It also requires a sound knowledge on physics processes occurring in the plant. The main difficulty when building such a model is the important entangling of physics processes and control activities. The model proposed by the first phases of MKSM address that problem by separating the two point of views, building on the one hand, the domain model which is a set of processes and on the other hand, the activity model representing the control operations on the plant. However, if the first step is to separate the two point of views, the second step identifies and defines the links between them.

The analysis leading to the model is a refining activity, guided by the pertinence of the concepts and not by the irreducibleness of the different elements. The details of what occur or how it occurs is not important if the model is sufficient to rightly apprehend the plant control. The model structure, i.e. the links between the different concepts in the model, is constructed progressively when building in parallel the two models, domain and activity. The cohesion of the models is guaranteed by this structure. The models take sense only when the whole set of links is established. There is no exhaustion in the describing of processes or control activities. The description is only sufficient for understanding and justifying the nuclear power plant management.

Our work is strongly based on the preliminary studies validating the State-oriented Approach principles. These studies have pointed out the importance of having the actual plant activity settled as a basis for building the control approach. The studies have led to the design of a thermo-hydraulic diagram describing the processes of transportation and evacuation of the reactor core energy. This diagram leads to the design of control rules based on six fundamental safety functions. This is an illustration of the strong dependence between the State-oriented Approach and the plant activity. The first experiences on the APE procedures brought up some evolutions we have included in our models. Due to the complexity of the involved phenomena, a large discussion for completion and validation has been performed with the experts of the Nuclear Safety Department of EDF.
We have also started to build the task model, which is part of the following phases of MKSM. The purpose was to identify and demonstrate the links between the previous models and the operational tasks performed by the plant operators, on a particular example only. Activity model gives the general and fundamental safety functions, and the task model gives the way to perform these functions. To build this example, we have been using these procedures written in the usual available documents for operators. Those procedures were only rewritten in the task language, which allows to enhance the strategy used to perform a given control activity.

3.2. Modelling the processes

The domain model for incidental and accidental states comprises 29 processes. This model has been considered as exhaustive, as far as it covers the whole set of phenomena identified up to now, and useful to the comprehension of incidental and accidental NPP control. This model has been discussed and validated by the Nuclear Safety Department of EDF. An example is given in figure 1.

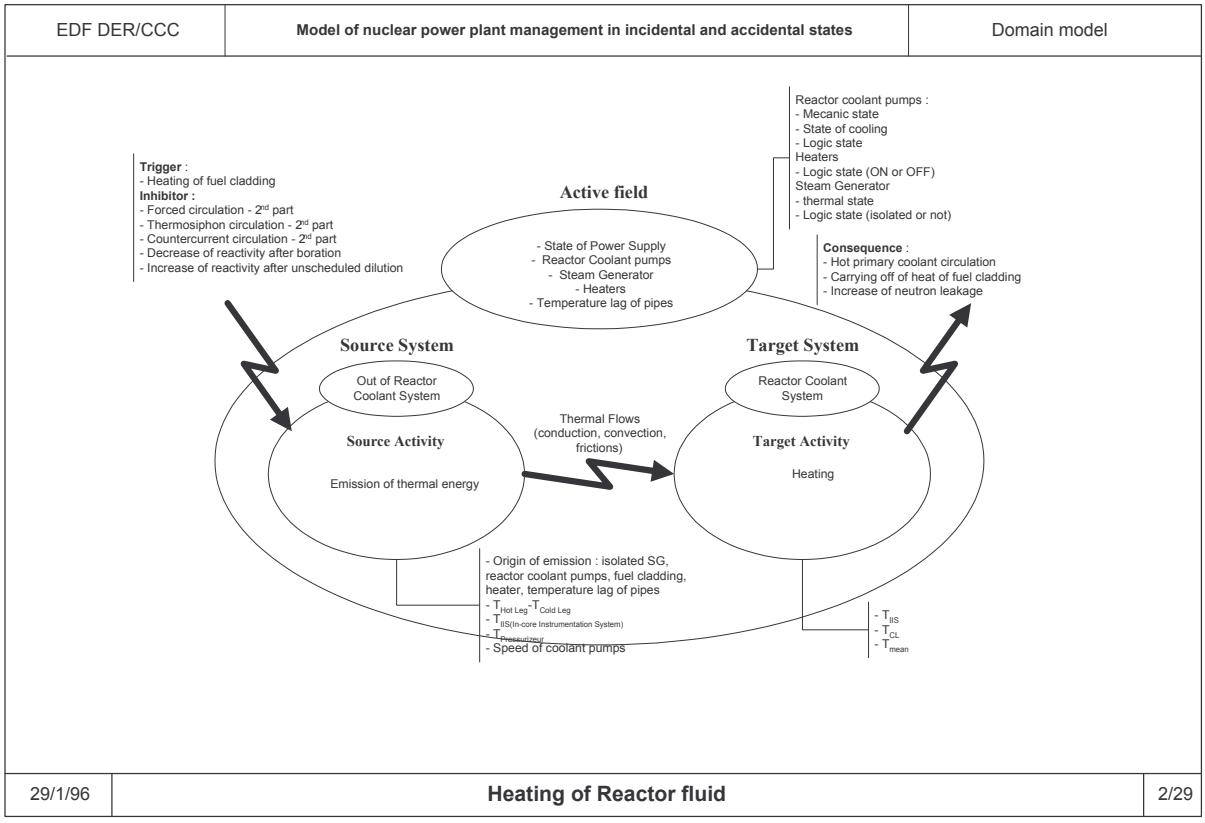

Fig. 1 : Example of process model

3.3. Establishing the scenarios

Scenarios design establishes the possible ways of chaining the processes of the domain together. Links between processes are causality relationships of two types : triggering or inhibiting. The set of those links, representing the different possible scenarios, gives the dynamic aspect of the processes involved. It covers the physics feedback loop involved in the operating control.

The analysis of that model shows the strong relationships between processes in a nuclear plant. An interesting point is that one can distinguish in the graph of scenarios three main components, "weakly connected", which correspond to the three fundamental safety principles in APE : confining, reactivity control, and core cooling. This is an a posteriori justification of those principles. An extract of the scenarios graph is given in figure 2.

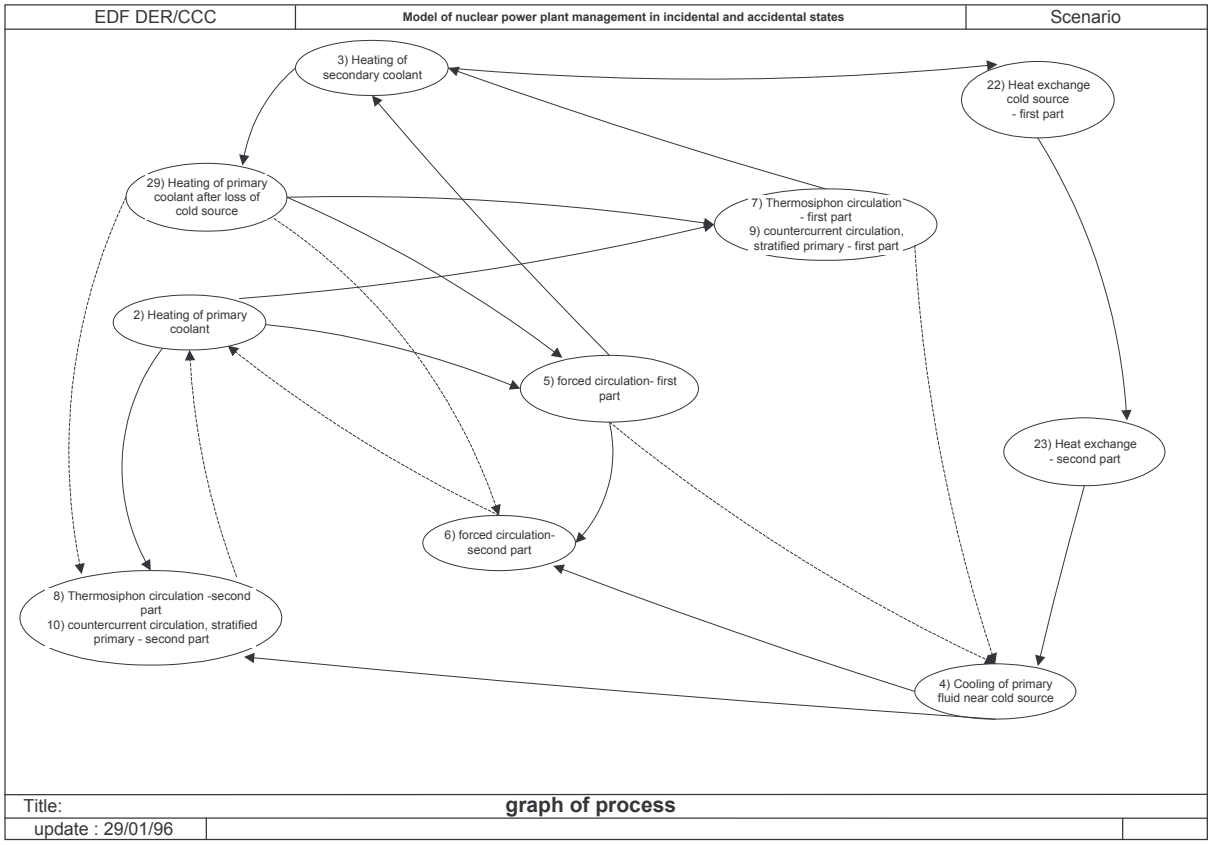

Figure 2 : Extract of the graph of processes

Processes and scenarios give an exhaustive view of all physics behaviours of the plant identified until now. The model is of great cognitive value because it is synthetic and reliable.

3.4. Modelling the activities

The goal of this model is to have a comprehensive view on all the possible control activities. This is a functional point of view on NPP control. As in the domain model, only activities allowing a better understanding of incidental and accidental NPP management are considered.

An activity describes what is possible to do to handle processes and reach a particular control objective. It is time independent. It initiates a transformation from a plant state to another. In addition to this transformation, an activity indicates the different acting operators, the equipment used in each activity, and the knowledge useful to correctly perform the actions. The hierarchy decomposing the activities exhibits the three fundamental safety functions (see above) but also, in a more detailed level, the six state functions essential in the APE [Depond 93].

A major interest in the activity model is that links have been established with the domain model :

*) Processes can be viewed as knowledge resources in checking activities. It means that the knowledge of the indicated processes is useful or necessary to correctly understand the checking activity.

*) Processes can be triggered by activities.

*) Processes can be inhibited by activities.

The last two links are very important in understanding and validating the control activities. In fact the complexity of NPP control (as for any industrial plant) comes from the fact that any action simultaneously triggers and inhibits different processes. By following the graph of processes, we can then check that for any scenario, there is a sequence of safety actions able to control it.

An example of the activity model is given in figure 3.

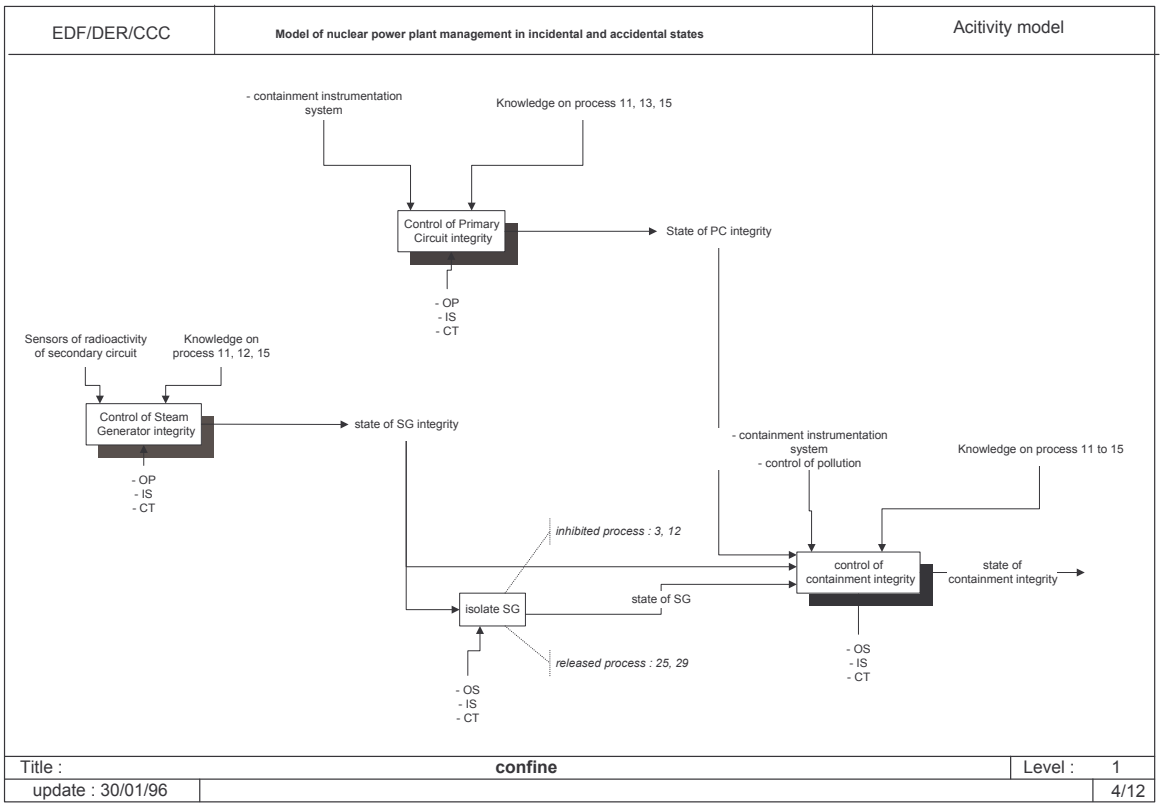

Figure 3 : Example of activity model

3.5. To the safety control procedures

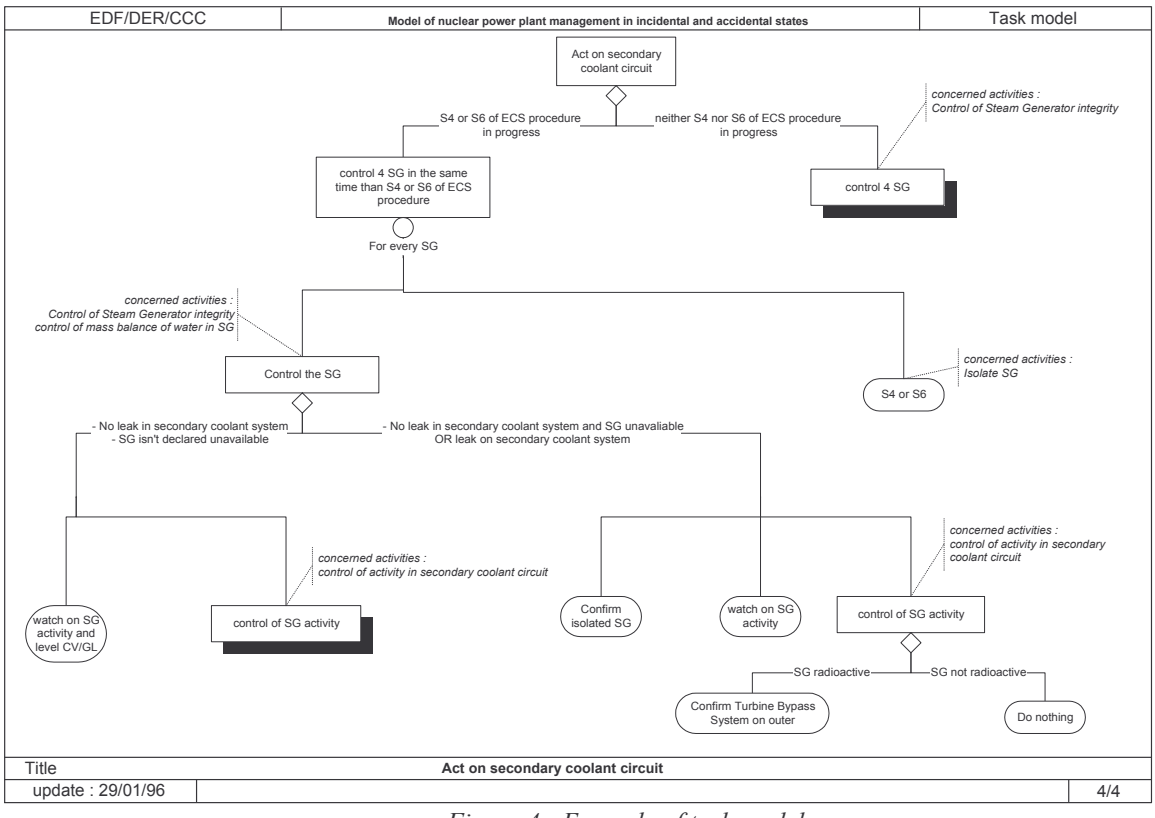

Figure 4 : Example of task model

Activity model is a general view over control actions. Operators in NPP are used to safety procedures, and it is necessary to link those general activities to these detailed procedures. In terms of MKSM modelling activity, it means to refine the activity model into a task model.

The two differences between the two models, are first that the « knowledge grain » is more refined in the task model which is a cognitive view over the knowledge system, compared to the domain model which is a contextual view, and second that the task model is control driven, compared to the model domain which is data driven.

In fact task model in NPP control describes what are the actual actions performed to achieve a goal given by an activity. Hence, it is based on the operator's procedures. The task model has been built by a simple reformulation of the safety procedures of the usual textbooks. The task language of MKSM was easy to use for that purpose. An example is given in figure 4. The whole set of procedures linked to the activity model has not been rewritten, because of the great number of tasks to write. It was on purpose for feasibility demonstration.

4. The hypermedia software

Starting from the results of modelling, it is pertinent to implement hypermedia software for computer-aided reading supports. The basic idea is to provide multiple access methods for learners.

4.1 Objectives

The purpose of the hypermedia application is to assemble the different knowledge models in order to offer an electronic version of what we can call a "knowledge book". This electronic knowledge book will be presented to operators in a training session. The operators will browse through this hypermedia instructional environment to learn about the complexity of NPP control.

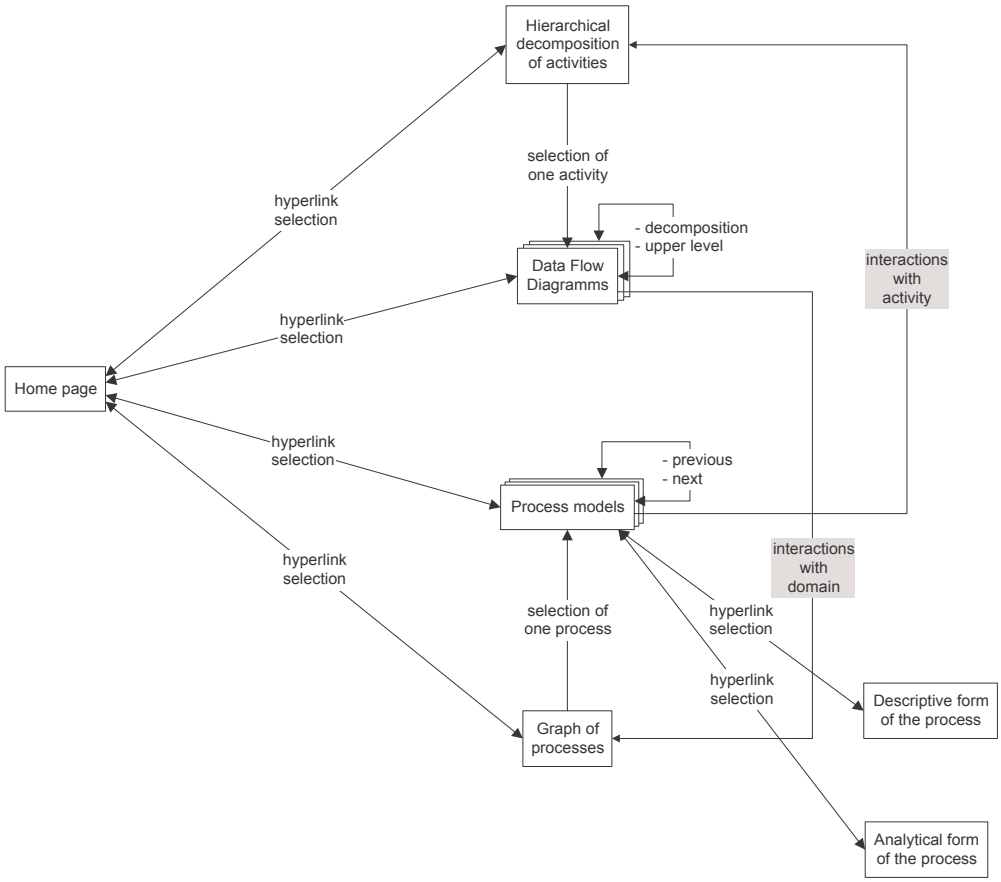

Figure 5: Hypermedia navigation

There are three main usages of the electronic knowledge book:

- Domain exploration: This usage concerns the understanding of the 29 processes involved in incidental and accidental states. It proceeds by browsing through the processes models in combination with the graph of scenarios. For one process, a descriptive form and an analytical form are proposed to give more comprehension.

- Activity exploration: Likewise, the operator is enabled to explore the data flow diagrams which describe the control activity. All these DFD are compiled in the tree of hierarchical functional decomposition.

- Interaction exploration: This is the main target of the educational environment. By selecting a given control activity, the operator can have access to all the processes that are involved in this activity. They are identified by meaningful coloration of the corresponding nodes in the processes graph. Conversely, the selection of one process allows identifying all the activities which trigger, inhibit or require the knowledge of this process.

4.2 Methodology for hypermedia design

Hypermedia applications typically include complex information, and may allow sophisticated navigation behaviour. Therefore designing hypermedia application differs from traditional software development. So specific methodologies are available to guide the design of such applications: RMM [Isakowitz 95], HDM [Garzotto 93], and DHRM [Halasz 94]. They differ in several ways. The HDM model provides an extensive and formal definition of meaningful hypermedia abstraction. The particular emphasis of RMM is on navigational and abstract interface design. DHRM primarily concentrates on the links physical definition and localisation. Because our material (knowledge models) is highly structured, we used a combination of those methodologies in a more practical and less ambitious way. According to RMM, the contents were modelled as in database design using the entity-relationships model. The navigation links were specified in finite states automata, the node of which is the various models.

4.3 Implementation and perspectives

The application was implemented using a commercial author language (Toolbook 3.0 from Asymetrix). Due to the amount of information in the graphical models, it was inconvenient to display more than only one graph at the same time. For this reason, the learner is unable to explore a process model and to check its position in the processes graph simultaneously. Consequently, to find the context of his state he has to select the hyperlink which goes back to the graph of scenarios.

For this kind of electronic book, the main problem arises with the maintenance of the application. Due to the fact that each hyperlink is specifically implemented in Toolbook, it is very expensive to assure the coherence of the navigation graph according to the content. We are looking for a hypermedia tool which allows the designer to maintain the application as data are updated.

5. Conclusion

The model which has been built in that project is a basis for a new control system in NPP. It is the minimal level of modelling for describing the plant control.

Using that model, it is possible to explain the physics processes taking place on a plant, and the activities necessary for its control. When integrating the operator's tasks in the model, it is possible to justify an action to perform by putting it in the context of processes and activities.

The number of links between models is considerable. So, the programming of hypermedia software enables to navigate more easily through the different point of views, and to establish pertinent chaining between the operator's tasks, control activities and physics processes. That software will be used for operator's training.

6. References

[Breuker 1994] Breuker J., Van de Velde W. Eds *: CommonKADS Library for Expertise Modelling*, IOS Press, 1994

[Depond 93] Depond G., Niger D. *: Synthèse des notions de base et principes généraux de l'APE pour la conduite incidentelle et accidentelle du REP*, D4002.46.1 SN/93/074, 1993

[Ermine 96] J.-L Ermine, M. Chaillot, P. Bigeon, B. Charreton, D. Malavieille : *MKSM, méthode de gestion des connaissances* (to appear)

[Garzotto 95] *Hypermedia design, analysis and evaluation issues* F. Garzotto, L.

[Halasz 94] *The Dexter hypertext reference model* F. Halasz, M. Schwartz. Com of the ACM, Vol 37, No 2, February 1994.

[Hickman 89] Hickman F.R., Killin J., Land L., Mulhall T., Porter D., Taylor R.M. : *Analysis for Knowledge-based Systems, a Practical Guide to the KADS Methodology*, Ellis Horwood, 1989

[Isakowitz 95] *RMM : A methodology for structured hypermedia design* Com of the ACM, Vol 38, No 8. August 1995.

[Le Moigne 77] Le Moigne J.-L. : *La théorie du Système Général, théorie de la modélisation*, P.U.F., Paris, 1977, 3ième édition mise à jour, 1990

[Scapin 90] : Scapin D., Pirret-Golbreich C. : *Towards a method for task description : Mad* , in L. Berlinguer and D. Berthelette (Eds), *Work in display units 89*, Elsevier Science Publishers, North Holland, 1990

[Sebillotte 88] Sebillotte S. : *Hierarchical planning as method for task analysis : the example of office task analysis*, Behaviour and information technology, vol. 7, n° 3, pp. 275-293, 1988